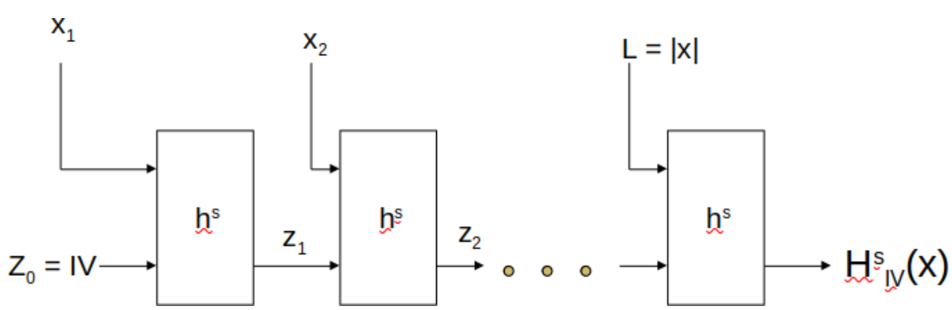
Task 7

Merkle-Damgard transform is way of extending a fixed length collision resistant hash function into a general one that receives inputs of any variable length. This method therefore transforms the problem of defining collision resistant hash functions that take an arbitrary input length and compress it to a fixed length to instead fixed length collision resistant hash functions that take a fixed length input and compress it to a fixed length output.

Build Algorithm



Let h^s be the fixed length collision resistant hash function which for inputs of length 2n gives an outputof length n.
The Merkle-Damgard transformation works as follows:

1) IV i.e. Z0 is defined which is just zeroes of the same length as taken by fixed length hash function with 1st block of message.
2) The inputs are sent as x1 and x2 for the fixed length hash functions. The output of the hash function is treated as one of the input for the next block.
3) This process continues till we calculate hash on each message block.
4) Finally, the message length that was calculated is appended as the final block and the final hash calculated is treated as the final output.

$Z_i = h^s (Z_{i-1} \,||\, x_i)$ and Z_{B+1} is obtained as the output

Proof

Theorem – If h is a fixed length collision resistant hash function, then H is also a collision resistant hash function.

We show that for any s, a collision in H yields a collision in h. Let x and x' be two different strings of respective lengths L and L' such that H(x) = H'(x'). Let x1 …. xB be the B blocks of padded x, and let x1'.. x'b, be the B' blocks of the padded x'. We have two possible cases:

1) **L != L'**: In this case, the last step of the computation of Hs(x) is z = h(zB || L) and of Hs(x0) is z = h(zB' || L'). Since H(x) = H(x') it follows that h(zB || L) = h(zB' || L'). However, L != L' and so hB || L and hB' || L' are two different strings that collide for h.

2) **L = L'**: Let zi and zi' be the intermediate hash values of x and x' during the computation of H(x) and H(x'), respectively. Since x != x' and they are of the same length, there must exist at least one index i (with 1 ≤ i ≤ B) such that xi != x'i. Let i∗ be the highest index for which it holds that zi∗-1 || xi∗ != zi'∗-1 || x'i∗.

If i∗ = B then (zi∗-1 || xi∗) and (zi'∗-1 || x'i∗) constitutes a collision because we know that H(x) = H(x') and L = L' implying that that zB = zB' . If i∗ < B, then the maximality of i∗ implies that zi∗ = zi'∗. Thus, once again, (zi∗-1 || xi∗) and (zi0∗-1 || x0i∗) constitutes a collision. That is, in both cases, we obtain that

zi∗-1 || xi∗ != zi'∗-1 || x'i∗

while,

h(zi∗-1 || xi∗) = h(zi'∗-1 || x'i∗);

meaning that there exists a collision in h. Therefore, we have shown that any collision in H follows a collision in h.

Since, we have already proven that h is collision resistant, therefore, this implies that H must also then be collision resistant.